

User Guide

Vexira Antivirus for Samba Servers





TABLE OF CONTENTS

VEXIRA ANTIVIRUS FOR SAMBA SERVERS	3
System requirements	3
Minimal required Linux distributions	3
Supported Samba versions	3
Installation, uninstallation	4
Operation.....	4
Configuration settings	6
General settings.....	6
Notification	7
Available tokens for messages	8
Registration data.....	8
Including external configuration file	8
Updating database	9
END USER AGREEMENT	10
CONTACT	12



VEXIRA ANTIVIRUS FOR SAMBA SERVERS

The program ensures comprehensive virus protection for Samba file servers on computers provided with Linux or Solaris operating system. The on access protection keeps the computer virus free. It works totally transparent mode, scans the files in the background, users don't perceive its operation.

The program is divided into two modules:

- shield module, which performs the scanning functions
- vfsemu module, which is an interface for the different Samba version

System requirements

```

=====
OPERATING |      Linux      | Sun Solaris 7
SYSTEM    | GLIBC 2.2.5    | (SunOS 5.7)
          | kernel2.2.1    |
=====
PROCESSOR | Intel Pentium  | Ultra Sparc
          | (or compatible)| Iie at 500MHz
          | at 300MHz      |
-----
MEMORY    |      64M*      |      128M*
-----
HARD DISK |                |      32M
-----

```

*Besides the basic memory requirement, the product needs ~25 MB extra memory for every connection to the Samba server.

Minimal required Linux distributions

- SuSE 8.0
- RedHat 7.3
- Debian 3.0 (woody)
- Mandrake 9.0
- Slackware 8.1

Supported Samba versions

Samba 2.2.1 - 3.0.23

Remark:

Those Samba versions that are newer than the mentioned above may be supported if their VFS module interface is compatible with the earlier versions.
 The 2.2.1-2.2.3 versions are only supported if the Samba daemon's binary was built with exported symbols.
 3.0 alpha XY versions are not supported.



Installation, uninstallation

The following package formats are available:

Linux

- RPM (redhat package)

Installation:

```
rpm -i vasambashield-<version>-<platform>.rpm
```

Uninstallation:

```
rpm -e vasambashield
```

- DEB (debian package)

Installation:

```
dpkg -i vasambashield-<version>-<platform>.deb
```

Uninstallation:

```
dpkg -r vasambashield
```

- TAR.GZ (general packed package)

Unpacking:

```
tar -xzvf vasambashield-<version>-<platform>.tar.gz
```

Installation:

```
vasambashield.install
```

At the beginning of the installation process the user must confirm the launching of the installation (y) and the program will be installed after accepting License Agreement (y).

Uninstallation:

```
vasambashield.remove
```

At the beginning of the uninstallation process, you have to confirm the launch of uninstallation (y).

Solaris

- PKG (Sun package)

Unpacking:

```
gunzip vasambashield-<version>-<platform>.pkg.gz
```

Installation:

```
pkgadd -d vasambashield.install-<version>-<platform>.pkg
```

Uninstallation:

```
pkgrm VAsambashield
```

- TAR.GZ (general packed package)

Use in the same way as described at Linux!

Operation

To activate the virus protection, the user has to modify the Samba's configuration file.

Setting of the various versions is differ:

In case of 2.x.y Samba version:

vfs object = <vfs module's name with path>



(specify absolute path)

In case of 3.x.y Samba version:

`vfs objects = <vfs module's name with path>`

or

`vfs objects = <vfs module's name>`

If this option already has parameter in the configuration file then the required line must be inserted to the previous ones.

The options above can be specified generally for all the shares (the option and its parameter must be placed in the [global] section) or for certain shares (the option and its value must be placed into the required share(s)).

Examples:

`vfs object = /usr/lib/samba/vfs/vasambavfsemu.so`

or

`vfs objects = vasambavfsemu`

The program scans for viruses only on that connection that have been established after the configuration file's modification, the previous ones will not be concerned.



Configuration settings

The configuration file is located on the `/etc/vasambashield/general.conf` path.

Settings in the `[general]` section

General settings

killable_action

If the virus is killable one of the following actions can be performed.

Available values:

quarantine - moving to quarantine

delete - deleting file

kill - killing virus

rename - renaming file

skip - ignore incident

Default: kill

non_killable_action

If the virus is non-killable one of the following actions can be performed.

Available values:

quarantine - moving to quarantine

delete - deleting file

rename - renaming file

skip - ignore incident

Default: skip

suspicious_action

In case of suspicious file is found, one of the following actions can be performed.

Available values:

quarantine - moving to quarantine

delete - deleting file

rename - renaming file

skip - ignore incident

Default: skip

scan_method

Specifying scanning method.

Available values: strict/fast/full

Default: strict

heuristic_level

Specifying the level of the heuristics scanning.

Available values:

normal - normal level

off - heuristics off

high - high level

Default: normal

log_level

Log level setting.

Available values:

EMERG or 0

ALERT or 1

CRIT or 2

ERR or 3

WARNING or 4

NOTICE or 5

INFO or 6



DEBUG or 7
DEBUG0 or 7
DEBUG1 or 8
DEBUG2 or 9
DEBUG3 or 10
DEBUG4 or 11
DEBUG5 or 12
DEBUG6 or 13
DEBUG7 or 14
DEBUG8 or 15
Default: INFO

tmp_path

Location of the temporary files.
Default: /tmp

vdb_file

Location of the virus database descriptor file.
Default: /var/lib/vasambashield/vdb9.xml

quarantine_path

Location of the quarantine directory.
Default: /var/spool/vasambashield/quarantine

virus_log_path

Location of the virus-log file. This file stores the log events created during virus scanning.
Default: /var/log/vasambashield/VirusScan.log

log_path

Location of the log file. This file stores the log events created during the program's operation.
Default: /var/log/vasambashield/general.log

file_log

Using log-file (yes/no).
Default: yes

samba_log

Using Samba log-system (yes/no).
Default: yes

syslog

Using syslog (yes/no).
Default: no

access_on_error

Allow or deny access to the file if error(s) occurred during the scan.
Values: allow/deny

Notification

message_sender = Samba Shield

Message sender's name.

message_virus_killed = "Message"

Sent message in case of virus found and killed. It must be specified between quotes, you can use tokens in the text.

message_access_denied = "Message"



Sent message in case of virus found but any error occurred. It must be specified between quotes, you can use tokens in the text.

Available tokens for messages

%virus%

Last found virus name.

%file%

The scanned file's name.

%version%

SambaShield version number.

Registration data

registration-username =

Enter user name.

registration-key =

Enter registration key.

Including external configuration file

It is possible to include external configuration files into the main configuration file. These linked files will be processed as a part of the main configuration file.

The architecture of external configuration files must be the same as the original, use the @ sign to specify external link to a file in the main configuration file.

Example:

@messages.conf.en

The default configuration file includes external file, too, linking messages sent in case of virus incident. It is practical to change the language of warning messages easily and quickly.



Updating database

The virus database updating could be performed manually or by update script automatically.

The product uses incremental virus database update mechanism to keep the virus database up-to-date. The advantage of this method is that the program doesn't need to download the whole virus database file every time (its size is several MBs) but usually only a small additional database package including the virus signatures processed and released recently. Using this mechanism, the download time is decreased to a minimal level so we can release additional virus database packages several times a day to improve the defense. Users can obtain protection against new malware without spending long time and generating considerable network load for the update. The protection is available almost immediately after the signatures of the newly discovered viruses have been processed in our virus lab.

Manual update

Our virus database-set consist of several files, you need to update all the files from our FTP server from the following folder and copy them to the virus database folder (/var/lib/vasambashield):
upd.vexira.com/pub2006/vexira/vdb.9/

Automatic update

We created a script to automate the update process, it is in the /usr/lib/vasambashield directory (vdbupdate.sh).

It is going to download the virus database, copies it into the correct directory. Updating will only be performed, if the database available in the server is newer than one installed on your computer. Otherwise the database will be left unchanged.

To execute the scripts, you should enter the
usr/lib/vasambashield.sh
command.

It is possible to use parameters, too:

--ftp

Download through FTP.

--http

Download through HTTP.

-v --verbose

Displays progress bar

-h --help

Displays help screen.

To run the script, you need wget program! With the help of cron, you can schedule the script executing to be performed by half an hours. Register into /etc/crontab:

```
0,30 * * * * root /usr/lib/vasambashield/vdbupdate.sh
```

If you have firewall and need using proxy server to get the outside network, see the wget manual about proxy settings.



END USER AGREEMENT

IF YOU DO NOT AGREE TO THESE TERMS AND CONDITIONS DO NOT INSTALL OR USE THE VEXIRA ANTIVIRUS SOFTWARE (referred to hereafter as the "Software"). BY CLICKING "YES", "I ACCEPT", "I AGREE", "OK", "CONTINUE", "NEXT" OR BY INSTALLING OR USING THE SOFTWARE IN ANY WAY, YOU ARE INDICATING YOUR COMPLETE UNDERSTANDING AND ACCEPTANCE OF THE TERMS AND CONDITIONS OF THIS END USER SOFTWARE LICENSE AGREEMENT (referred to hereafter as the "License"). IF YOU DO NOT ACCEPT ALL OF THE TERMS AND CONDITIONS OF THIS LICENSE, THEN CENTRAL COMMAND, INC. IS UNWILLING TO LICENSE THE SOFTWARE TO YOU. YOU MAY, WITHIN THIRTY (30) DAYS OF YOUR INITIAL PURCHASE OF A COPY OF THE SOFTWARE, RETURN THE ENTIRE COPY OF THE SOFTWARE (INCLUDING ALL COMPUTER MEDIA, PACKAGING AND DOCUMENTATION) WITH PROOF OF PURCHASE EITHER TO CENTRAL COMMAND, INC. DIRECTLY AT ITS CUSTOMER SERVICE DEPARTMENT OR TO THE RETAILER FROM WHICH YOU PURCHASED THE SOFTWARE, FOR A FULL REFUND OF THE AMOUNT INDICATED BY YOUR SALES RECEIPT OR PROOF OF PURCHASE FOR THE SOFTWARE.

IF YOU ARE INSTALLING THE SOFTWARE ON A COMPUTER THAT IS NOT OWNED BY YOU, YOU ARE BOUND TO THE TERMS AND CONDITIONS OF THIS LICENSE BOTH IN YOUR INDIVIDUAL CAPACITY AND AS AN AGENT OF THE OWNER OF THE COMPUTER, AND YOUR ACTIONS WILL BIND THE OWNER OF THE COMPUTER. YOU REPRESENT AND WARRANT TO CENTRAL COMMAND, INC. THAT YOU HAVE BOTH THE CAPACITY AND AUTHORITY TO ENTER INTO THIS LICENSE ON YOUR OWN BEHALF AS WELL AS ON BEHALF OF THE OWNER OF THE COMPUTER ON WHICH YOU ARE INSTALLING THE SOFTWARE. FOR PURPOSES OF THIS LICENSE, THE "OWNER" OF A COMPUTER IS THE INDIVIDUAL OR ENTITY THAT HAS LEGAL TITLE TO THE COMPUTER OR THAT HAS THE POSSESSORY INTEREST IN THE COMPUTER IF IT IS LEASED OR LOANED BY THE ACTUAL TITLE OWNER.

This End User License Agreement ("License") is a legal agreement between you (either an individual, agent of the owner, or a single entity end user) and Central Command, Inc. for use of the Central Command, Inc. software product identified above (i.e. Vexira Antivirus), which includes computer software and may include associated media, printed materials, and "online" or electronic documentation (collectively referred to as the "Software"), all of which are protected by U. S. copyright laws and international treaty protection. By installing, copying, or otherwise using the Software, you agree to be bound by the terms of this License. If you do not agree to the terms of this License, do not install or use the Software.

The Software and the name "Vexira Antivirus" is protected by copyright laws and international copyright treaties, as well as other intellectual property laws and treaties. The Software is licensed, not sold. If you agree to be bound by all of the terms of this License, you will only own the media on which the Software has been provided and not the Software itself.

THIRTY DAY MONEY BACK GUARANTEE: If you are the original licensee of this copy of the Software and are dissatisfied for any reason with it within the first thirty (30) days after your purchase or delivery date, you may return the complete product, together with your original proof of purchase to Central Command, Inc. or the retailer from which you purchased the Software, for a refund of the amount indicated by your original proof of purchase. If this purchase was completed using electronic delivery you are required to complete a Letter of Destruction (referred to hereafter as an "LOD") and return it within thirty (30) days after your purchase date to receive a refund. Central Command, Inc. uses the postmark or fax date of the completed and returned LOD to determine compliance. You can receive a LOD by contacting your electronic retailer from which you purchased the software or directly from Central Command, Inc. via e-mail at service@centralcommand.com, postal mail at P.O. Box 468, Medina, Ohio, 44256, or fax at +1 330-722-6517. For assistance you may also contact Central Command, Inc. by calling +1 330-723-2062 and requesting Customer Service.

GRANT OF LICENSE: Central Command, Inc. hereby grants you and only you a non-exclusive license to use the Software subject to and upon all of the terms and conditions set forth in this License.

APPLICATION SOFTWARE: You may install and use only one copy of the Software, and only on a single computer terminal.

NETWORK USE: You may also store or install a copy of the Software on a storage device, such as a network server, which is used only to install or run the Software on your other computers over an internal network; however, you must purchase and dedicate a separate license for each separate computer terminal on which the Software is installed or run from the storage device. A license for the Software may not be shared or used concurrently on different computers or computer terminals. You are required to purchase a license pack or multi-use license if you require multiple licenses for use on multiple computers or computer terminals.

If you purchase a License Pack and you have acquired this License for multiple licenses of the Software, you may make the number of additional copies of the computer software portion of the Software specified above as "Licensed copies." You are also entitled to make a corresponding number of secondary copies for use on a single home computer as specified above in the section entitled "Application Software".

If you purchase a License for the Software to be used to virus scan electronic messages or you install the Software in such a way to virus scan electronic messages you are required to purchase a license for each domain name and each sub domain name that is virus scanned. If your total electronic mail addresses exceed 6000 you are required to purchase a special Internet



Vexira Antivirus for Samba Servers

Service Provider (ISP) License for use of the Software.

TERM OF LICENSE: The License granted hereunder shall commence on the date that you install, copy or otherwise first use the Software. You may terminate this License at any time. This License shall terminate automatically (and you shall have no right to use the Software) upon your breach of any term of this License. Upon termination, you must destroy the Software and all copies, if any, you made pursuant to this License.

UPGRADES: If the Software is labeled as an upgrade, you must be properly licensed to use a product identified by Central Command, Inc. as being eligible for the upgrade in order to use the Software. A copy of the Software labeled as an upgrade replaces and/or supplements the product that formed the basis for your eligibility for the upgrade. You may use the resulting upgraded product only in accordance with the terms of this License. If the Software is an upgrade of a component of a package of software programs that you licensed as a single product, the Software may be used and transferred only as part of that single product package and may not be separated for use on more than one computer.

COPYRIGHT: All right, title and interest in and to the Software and the name "Vexira Antivirus" and "Vexira" and all copyright rights in and to the Software (including but not limited to any images, photographs, animations, video, audio, music, text, and "applets" incorporated into the Software), the accompanying printed materials, and any copies of the Software are owned by Central Command, Inc. and/or its suppliers. The Software is protected by copyright laws and international treaty provisions. Therefore, you must treat the Software and the term "Vexira Antivirus" or "Vexira" like any other copyrighted material except that you may install the Software on a single computer provided you keep the original solely for backup or archival purposes. You may not copy the printed materials accompanying the Software. You may not use the name "Vexira Antivirus" or "Vexira" or any similar name except when referring to the Software. You must produce and include all copyright notices in their original form for all copies created irrespective of the media or form in which the Software exists. You may not sub-license, rent, sell, or lease the Software. You may not reverse engineer, recompile, disassemble, create derivative works, modify, translate, or make any attempt to discover the source code for the Software or any part thereof. Except as expressly permitted by applicable law, you may not remove from the Software, or alter, any of the trademarks, trade names, logos, patent or copyright notices or other proprietary rights notices or markings, or add any other notices or markings to the Software.

LIMITED WARRANTY: Central Command, Inc. warrants that the media on which the Software is distributed is free from defects for a period of thirty (30) days from your date of receipt or purchase date of the Software. Your sole remedy for a breach of this warranty will be that Central Command, Inc. at its option, may replace the defective media upon receipt of the damaged media, or refund the money you paid for the Software. Central Command, Inc. does not warrant that the Software will be uninterrupted or error free or that the errors will be corrected. Central Command, Inc. does not warrant that the Software will meet your requirements. CENTRAL COMMAND, INC. HEREBY DISCLAIMS ALL OTHER WARRANTIES FOR THE SOFTWARE, WHETHER EXPRESSED OR IMPLIED. THE ABOVE WARRANTY IS EXCLUSIVE AND IN LIEU OF ALL OTHER WARRANTIES, WHETHER EXPRESSED OR IMPLIED, INCLUDING THE IMPLIED WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE, OR NON-INFRINGEMENT. THIS WARRANTY GIVES YOU SPECIFIC LEGAL RIGHTS. YOU MAY HAVE OTHER RIGHTS, WHICH VARY FROM STATE TO STATE.

DISCLAIMER OF DAMAGES: Anyone installing, using, testing, or evaluating the Software bears all risk to the quality and performance of the Software. In no event shall Central Command, Inc. be liable for any damages of any kind, including, without limitation, direct, indirect, exemplary, special, consequential or incidental damages of any kind (including without limitation lost profits or damage to other systems) arising out of the use, performance, or delivery of the Software, even if Central Command, Inc. has been advised of the existence or possibility of such damages. SOME STATES DO NOT ALLOW THE LIMITATION OR EXCLUSION OF LIABILITY FOR INCIDENTAL OR CONSEQUENTIAL DAMAGES, SO THE ABOVE LIMITATION OR EXCLUSION MAY NOT APPLY TO YOU. IN NO CASE SHALL CENTRAL COMMAND, INC.'S LIABILITY EXCEED THE PURCHASE PRICE PAID BY YOU FOR THE SOFTWARE. The disclaimers and limitations set forth above will apply regardless of whether you accept or use, evaluate, or test the Software.

IMPORTANT NOTICE TO USERS: THE SOFTWARE IS NOT FAULT-TOLERANT AND IS NOT DESIGNED OR INTENDED FOR USE IN ANY HAZARDOUS ENVIRONMENT REQUIRING FAIL-SAFE PERFORMANCE OR OPERATION. THIS SOFTWARE IS NOT FOR USE IN THE OPERATION OF AIRCRAFT NAVIGATION, NUCLEAR FACILITIES, OR COMMUNICATION SYSTEMS, WEAPONS SYSTEMS, DIRECT OR INDIRECT LIFE-SUPPORT SYSTEMS, AIR TRAFFIC CONTROL, OR ANY APPLICATION OR INSTALLATION WHERE FAILURE COULD RESULT IN DEATH, SEVERE PHYSICAL INJURY OR PROPERTY DAMAGE.

GOVERNMENT RESTRICTED RIGHTS/RESTRICTED RIGHTS LEGEND: Use, duplication, or disclosure by the Government is subject to restrictions as set forth in subparagraph (c)(1)(ii) of the Rights in Technical Data and Computer Software clause at DFARS 252.227-7013 or subparagraphs (c)(1) and (2) of Commercial Computer Software-Restricted Rights clause at 48 CFR 52.227-19, as applicable. Contact Central Command, Inc., at P.O. Box 468, Medina Ohio 44258-0468.

GENERAL: This License is deemed delivered in, and will be governed by, the laws of the State of Ohio, in the United States of America. This License may only be modified by a license addendum, which must accompany this License or by a written document which has been signed by both you and Central Command, Inc. This License has been written in the English language only and is not to be translated or interpreted in any other language. Prices, costs and fees for use of the Software are subject to change without notice to you. In the event of invalidity of any provision of this License, the invalidity shall not affect the validity of the remaining portions of this License. Vexira, Vexira logo, Central Command, Central Command's logo, EVRT, Emergency Virus Response Team, Without us, there's no defense, are trademarks of Central Command, Inc. Microsoft,



Vexira Antivirus for Samba Servers

Windows, Excel, Word, the Windows logo, Windows NT, Windows 2000 are registered trademarks of Microsoft Corporation. All other trademarks or tradenames are the property of their respective owners.

CONTACT

This manual provides comprehensive information on operational of our virus protection product. If you have any additional questions about it or would like to share your experience or proposals with us do not hesitate to contact us! Turn to us with confidence, your demands and remarks will be respected.

Address Central Command, Inc.
Medina, Ohio 44258,
P. O. Box 468.
United States

Phone (+1) 330 723 2062
Fax (+1) 330 722 6517
Web www.centralcommand.com
E-mail sales@centralcommand.com
support@centralcommand.com